IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF: **ONE BLACK APPLE IPHONE cellular "smart phone" with rubber case, IMEI 35 646210 602902 0, Serial Number FFWCG9AGPLJY;**	Magistrate No. 21-832

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

I, Jonathan K. DuThinh, a Special Agent with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), being duly sworn, depose and state that:

INTRODUCTION AND AGENT BACKGROUND

1. I have been employed as Special Agent with the ATF for approximately five (5) years. I am currently assigned to the ATF Pittsburgh Field Office, Group II. As part of my duties, I am authorized to conduct investigations of persons who engage in unlawful firearms possession, acquisition and use as well as violent crimes including commercial robberies.

2. I have been personally involved in dozens of firearms investigations, and as such I am familiar with the various methods used by prohibited persons to acquire firearms. I have experience with a wide range of investigative techniques, including various types of visual and electronic surveillance, the interception of wire communications, and the debriefing of defendants, witnesses and informants, as well as others who have knowledge of the distribution and transportation of controlled substances, controlled deliveries, use of search and arrest warrants, management and use of informants, pen registers, the laundering and concealing of proceeds from drug trafficking, and the street gangs who participate in these illegal activities.

3. This Affidavit is made in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for the issuance of a search warrant authorizing the search of property

– an electronic device – which is currently in law enforcement custody, and the extraction from that property of the electronically stored information described in Section II of Attachment A.

4. The information contained herein is based upon my own personal investigation, observations, and knowledge as well as upon the investigation, personal observations, and knowledge of other law enforcement officers with whom I have discussed this case. Because this Affidavit is being submitted for the limited purpose of establishing probable cause in support of a search warrant, I have not included every item of evidence or piece of information known to me; rather, I have included only those facts necessary to establish probable cause.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. This Application and Affidavit are being submitted in support of a search warrant for the following device, which is currently in the custody of the ATF at the Pittsburgh Field Office:

a. One Black APPLE IPHONE cellular "smart phone" with rubber case IMEI 35 646210 602902 0, Serial Number FFWCG9AGPLJY, recovered from the person of Abdullah WOODS by Duquesne Police Officer Johnston on December 8, 2020; currently secured with the ATF and hereinafter referred to as **TELEPHONE 1**.[1]

6. Investigators, including your Affiant, believe the records and other information contained within **TELEPHONE 1** contain evidence of violations of Title 18, United States Code, Sections 922 and 924, which make it unlawful for certain individuals to possess firearms and

1 On December 21, 2020, at Magistrate No. 20-2516, a search warrant for TELEPHONE 1was signed by Judge Lisa Pupo Lenihan. The description of the phone in the warrant at 20-2516 ("One White APPLE IPHONE cellular "smart phone" with rubber case, recovered from the person of Abdulah WOODS by Duquesne Police Officer Johnston on December 8, 2020") was derived from a Duquesne Police Report which erroneously specified the color of the phone as "white" (when it should have read "black"). The warrant at 20-2516 was not executed. Since that time, the phone was taken into ATF custody and the correct color and other identifiers now known to your Affiant are now included in the corrected description above.

prohibits the possession of firearms during and in relation to drug trafficking crimes and 21 USC 841 and 846, which prohibit the possession and distribution of controlled substances and conspiracy to do so (hereinafter referred to as the **TARGET OFFENSES**).

7. The applied-for warrant would authorize the forensic searches of **TELEPHONE 1** for the purpose of identifying electronically stored data particularly described in Section II of Attachment A.

FACTS RELATING TO PROBABLE CAUSE

8. On December 7, 2020, Law Enforcement Officers (LEOs) from the Duquesne Police Department (DPD) observed a light blue Dodge Grand Caravan commit a traffic violation and effectuated a traffic stop on said vehicle, which displayed PA registration LKD9639. LEOs made contact with the sole occupant and operator of the vehicle, later identified as Abdulah WOODS. WOODS provided LEOs with a Michigan driver's license, which he produced from a brown leather card holder that was in between his legs on the driver's seat. LEOs observed marijuana blunt roaches in the vehicle and requested WOODS from the vehicle. WOODS refused to exit and began arguing with LEOs. LEOs attempted to physically remove WOODS from the vehicle but were unsuccessful. During LEOs physical interaction with WOODS, WOODS was able to place the vehicle in drive and flee from LEOs. LEOs returned to their DPD vehicles and attempted to re-effectuate the traffic stop of WOODS' vehicle. LEOs observed WOODS travelling at a high rate of speed into the City of McKeesport, PA. Due to such, DPD LEOs terminated their pursuit and informed assisting McKeesport PD (MPD) LEOs of WOODS' direction of flight.

9. Assisting MPD LEOs familiar with WOODS knew of him to frequent apartment #14 Building of the Harrison Village Apartments in McKeesport. Furthermore, one of the assisting MPD LEOs had taken a report regarding WOODS on November 28, 2020, in which the reporting party informed LEOs that WOODS carries a firearm in a blue book bag with the word "Cookie" on it. LEOs travelled to the aforementioned apartment, where they observed WOODS' vehicle

parked in front, with smoke emanating from beneath the hood of the vehicle and the headlights still on. DPD and MPD LEOs established a perimeter and made contact with a female occupant, later identified as Mesha Woods, in the front doorway of the apartment. While LEOs were communicating their purpose for being at Mesha Woods' apartment, WOODS pushed past Mesha Woods towards LEOs. LEOs instructed WOODS to get on the ground. WOODS did so and was detained.

10. After WOODS was detained, Mesha Woods stated the light blue Dodge Caravan belonged to her sister-in-law. Mesha Woods confirmed that she knew WOODS, but did not grant him entry into her apartment, where she is the lessee. Mesha Woods completed a MPD Rights Warning and Voluntary Consent to Search form. Pursuant to the search of Mesha Woods' apartment, LEOs recovered a blue back pack with the word "Cookie" on it, on the ground floor closet of Mesha Woods' apartment. Within the back pack was an automobile key for the light blue Dodge Caravan bearing PA registration LKD9639, a brown leather card holder (previously viewed by DPD LEOs during the traffic stop) containing WOODS' debit card, work identification and health insurance card, two firearms (one Glock model 22 pistol and one Glock model 21 pistol), approximately 361 grams of suspected crack/cocaine, approximately 973 grams of suspected marijuana, and a sum of US currency. Located on WOODS' person was a black Apple iPhone cellular "smart phone" in a rubber case **(TELEPHONE 1)**.

11. Your Affiant is aware, through both training as well as experience gained through multiple narcotics investigations, that the targets of those narcotics investigations utilize cellular telephones to not only arrange meetings with their drug customers but also speak with fellow co-conspirators and their drug sources of supply. Your Affiant is also aware that these targets also utilize multiple cellular telephones at one time in an effort to not only thwart detection by law enforcement but also to compartmentalize their drug trafficking customers to one phone, their co-conspirators to another phone, and their drug source of supply to yet another phone.

12. Based upon my training and experience, I am aware that it is generally a common practice for drug traffickers to store the names and phone numbers of drug customers and photographs and videos detailing illegal activities in cellular telephones. Because drug traffickers in many instances will "front" (that is, sell on consignment) controlled substances to their clients, and/or will be "fronted" controlled substances from their suppliers, such record-keeping is necessary to keep track of amounts paid and owed, and such records will also be maintained close at hand so as to readily ascertain current balances. Often drug traffickers keep "pay and owe" records to show balances due for drugs sold in the past ("pay") and for payments expected ("owe") as to the trafficker's supplier(s) and the trafficker's dealer(s). Additionally, drug traffickers must maintain telephone and address listings of clients and suppliers and keep them immediately available in order to efficiently conduct their drug trafficking business.

13. Members of Drug Trafficking Organizations (DTO) often take group photographs with other enterprise members posing with paraphernalia, money and/or drugs. Many cellular telephones have a camera feature that is readily capable of capturing and storing these group photos. Moreover, in my experience, the phones of individuals who illegally possess firearms often contain evidence of unlawful firearm possession in the form of text messages, e-mails, and social media posts. It has also been my experience that such phones often contain information regarding how an unlawful possessor acquired his firearm.

14. Members of DTOs often store each other's phone numbers and contact information in the directories of their cellular phones.

15. Based on my experience and familiarity with cellular telephones, I am aware that the telephones have voicemail and telephone directory features, as well as camera features which allow the user to take photographs and store them in the cellular phone's memory card. Based on my experience and training, statements by other law enforcement officers, and personal observations, I know that because of the storage capacity of cellular telephones, the portability of

cellular telephones, the ease with which information stored on a cellular telephone may be accessed and/or organized, and the need for frequent communication in arranging narcotics transactions, cellular telephones are frequently used by individuals involved in drug trafficking. In particular, I and other law enforcement officers have found that information frequently maintained on cellular telephones includes the contact numbers of other co-conspirators, contact numbers for narcotics customers and stored photographs of DTO activities. This evidence will come in the form of caller identification information, call log information, telephone numbers, address information, or other identification information, as well as opened and unopened voicemail and/or text messages, photographs, videos and information about access to the Internet.

16. Members of DTOs routinely use multiple physical phones in succession as one breaks or the DTO feels that the number associated with the phone is compromised by law enforcement. The physical phone may no longer be an active communicative device, however many times these old phones are not discarded as they possess value to the DTO. The replaced device contains within it the contact information for drug customers of the DTO, and many times these phones are maintained as digital phone books should the new active phone become unusable or unavailable. Furthermore, these replaced phones are commonly kept in a relatively accessible location where either all or select members of the DTO can access the information within should it become necessary. As stated above, members of DTOs routinely take photographs and or memorialize other information of evidentiary value within these replaced phones. As such, it is common to recover a multitude of otherwise inactive phones especially at locations central to or important to the drug trafficker. Additionally, your affiant knows that persons who are legally prohibited from the purchase and possession of firearms acquire firearms through unlawful means. In order to do so, the solicitation and transaction thereof is often conducted via digital media devices and the conversations, pictures and specifics of the transaction are often stored within cellular devices.

Electronic Storage and Forensic Analysis

17. As described above and in Attachment A, Section II, this Application seeks permission to search **TELEPHONE 1** (hereinafter referred to as the **TARGET DEVICE**) for records that might be found on the **TARGET DEVICE**, which will evidence violations of the **TARGET OFFENSES**.

18. One form in which the records might be found is data stored on a cellular telephone.

19. Based on my knowledge, training, and experience, I know that files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.

20. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on an electronic device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

21. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, an electronic device's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

22. Wholly apart from user-generated files, electronic device storage media—in particular, electronic devices' internal hard drives—contain electronic evidence of how an electronic device has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Electronic device users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to

delete this information.

23. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

24. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

Forensic Evidence: Deleted Files, User Attribution

25. *Nature of examination*. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

26. *Manner of execution*. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

27. Based upon the foregoing, you Affiant submits that there is probable cause to believe the **TARGET DEVICE** contains information related to the **TARGET OFFENSES** which law enforcement has probable cause to believe have been committed by Abdullah Woods, and others both known and unknown.

/s/ Jonathan DuThinh
JONATHAN DuTHINH, Special Agent
Bureau of Alcohol, Tobacco, Firearms and Explosives

Sworn and subscribed to me, by telephone
pursuant to Fed. R. Crim. P. 4.1(b)(2)(A),
this 16th day of April, 2021.

HONORABLE MAUREEN P. KELLY
United States Magistrate Judge

ATTACHMENT A

I. Device to be Searched (TARGET DEVICE)

a. One Black APPLE IPHONE cellular "smart phone" with rubber case IMEI 35 646210 602902 0, Serial Number FFWCG9AGPLJY, recovered from the person of Abdullah WOODS by Duquesne Police on December 8, 2020; currently secured with the ATF Pittsburgh Field Office (**TELEPHONE 1)**.

II. Records and Other Information to Be Seized

1. All records, information, and items evidencing who used the device and/or when and/or from where, as well as evidence of violations of the following statutes including but not limited to Title 18 U.S.C. §§ 922 and 924 and 21 USC 841 and 846 on the **TARGET DEVICE**, including:

a. incoming and outgoing call and text message logs,
b. contact lists,
c. photo and video galleries,
d. sent and received text messages,
e. online searches and sites viewed via the internet,
f. online or electronic communications sent and received, including email, chat, and instant messages,
g. sent and received audio files,
h. navigation, mapping, and GPS files,
i. telephone settings, including speed dial numbers and the telephone number for the **TARGET DEVICE** and related identifying information such as the ESN for the **TARGET DEVICE**,
j. call forwarding information,
k. messages drafted but not sent, and
l. voice messages.

2. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored,

including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form. However, no real-time communications will be intercepted and searched during service.

3. In searching the **TARGET DEVICE**, federal agents may examine all of the data contained in the **TARGET DEVICE** to view its precise contents and determine whether the **TARGET DEVICE** and/or data falls within the items to be seized as set forth above. In addition, they may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth above.